อนิวรรตน์ สมาธิวัฒน์

ล้างอิทธิพลแฮกเกอร์ แค้นนี้ต้องชำระ

เรื่องราวของการแฮ็ก ปรากฏเป็นข่าวให้เห็นกันบ่อย ๆ หลายคนเชื่อว่า เป็นการสร้างสีสันให้กับข่าว ให้ดูตื่นเต้นเกินจริง หลายคนคิดว่าเป็นเรื่องไกลตัว หลายคนคิดว่าไม่เป็นเรื่องไร้สาระ และอีกหลายคน "เคยถูกแฮ็กมาแล้ว"

เมื่อเทคโนโลยีคอมพิวเตอร์กลายเป็นสิ่งจำเป็น ประสิทธิภาพงานที่เพิ่มขึ้น หมายถึงการลดต้นทุน ซึ่งจะส่งผลกระทบเป็นวงกว้าง ในขณะที่คู่แข่งมีการแรงปรับตัวตามเทคโนโลยี มิฉะนั้นจะไม่สามารถแข่งขันทั้งราคา และบริการ บริษัทขนาดเล็กอาจใหญ่ได้ในไม่กี่ปี และบริษัทยักษ์ใหญ่อาจล้มละลายได้ง่าย ๆ ดังนั้น ทุกบริษัทจึงหลีกเลี่ยงไม่ได้เสียแล้ว ในการที่จะนำคอมพิวเตอร์เข้ามาในการดำเนินธุรกิจ

อย่างไรก็ตาม การนำคอมพิวเตอร์เข้ามาก็ส่งผลเสียด้วยเช่นกัน ในการหาบุคลากรทางด้านคอมพิวเตอร์ ซึ่งหายาก ค่าตัวแพง มีค่าบำรุงรักษา รวมทั้งความซับซ้อนของเทคโนโลยี ซึ่งค่อนข้างเข้าใจยาก การนำเทคโนโลยีมาใช้โดยเข้าใจเพียงผิวเผิน อาจส่งผลดีในระยะสั้นกับองค์กร แต่ในระยะยาวย่อมเสี่ยงกับความเสียหายใหญ่หลวง หนึ่งในนั้นคือ ความเสียหายเนื่องจากระบบความปลอดภัยในข้อมูล

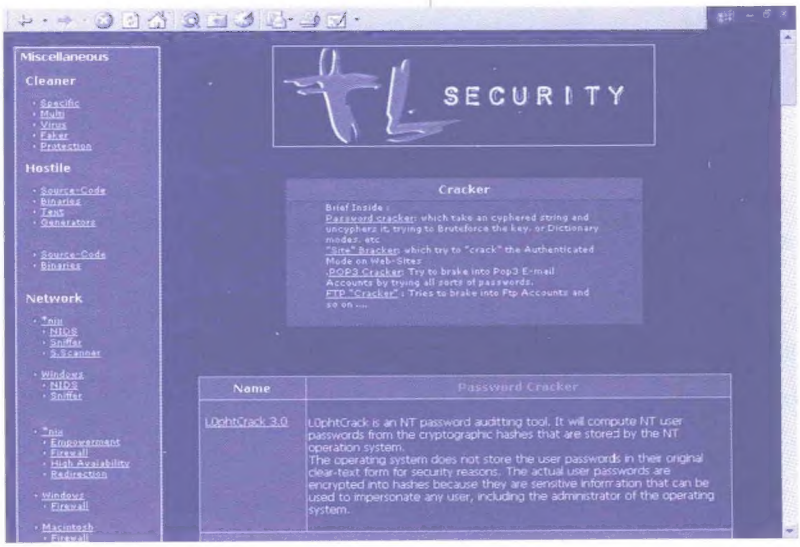
ความเสียหายเนื่องจากปัญหาระบบความปลอดภัยบนคอมพิวเตอร์นี้ มีจำนวนมากขึ้นเรื่อย ๆ ส่วนมากจะถูกปกปิดเพราะกลัวส่งผลกระทบกับการดำเนินงาน ทั้ง ๆ ที่เป็นที่รู้กันว่าตัวเลขที่เสียหายจริงมีจำนวนมากกว่าที่เป็นข่าวมาก

ในยุคที่ข้อมูลเป็นสิ่งมีค่าเช่นนี้ ทำให้ต้องให้ความสำคัญกับการปกป้องข้อมูลมากขึ้น หน่วยงานอาจได้รับความเสียหายเนื่องจากข้อมูลได้หลายวิธี ตั้งแต่ ข้อมูลลูกค้า ข้อมูลทางบัญชีการเงิน เทคโนโลยี และการวิจัย สูตรการผลิต และข้อมูลอื่น ๆ อาจถูกสำเนา ลบทิ้งทำลาย ส่งผลความเสียหายร้ายแรง ลองนึกภาพหากข้อมูลฝากถอนเงินของธนาคารเกิดเสียหาย แม้ธนาคารจะมีฮาร์ดก๊อบปี้ หรือเอกสารอยู่ก็ตาม แต่จะเป็นไปได้หรือที่จะมานั่งคีย์ข้อมูลใหม่นับล้านรายการต่อวันเข้าไป รวมทั้งตรวจสอบกันใหม่ ทั้งยังความผิดพลาดที่เกิดจากการคีย์ข้อมูล รวมถึงการที่ต้องหยุดกิจการเพื่อแก้ไขปัญหา หรือแม้แต่การที่คู่แข่งได้ข้อมูลสำคัญขององค์กรไป ดังที่เคยมีกรณีเช่นแฮ็กเกอร์ขโมยเลขบัตรเครดิตมาแจกบน อินเทอร์เน็ต

ผู้ที่อาจสร้างความเสียหายให้กับเราได้นั้น อาจไม่รู้จักกันเป็นการส่วนตัว หรืออาจจะเป็นคนใกล้ตัวก็ได้ ตั้งแต่เพื่อนบ้าน พนักงานในบริษัท คู่แข่งทางการค้า โกรธแค้น หมั่นไส้ อิจฉา มิจฉาชีพ ไปจนถึงมือสมัครเล่น อยากลองของ คุณยังอาจคิด

ว่าเป็นเรื่องยากสำหรับคนเหล่านี้ และดูจะเป็นเรื่องเพ้อเจ้อ ที่จะมีใครคิดจะมาขโมยหรือเปลี่ยนแปลงข้อมูลของคุณเหมือนอย่างในหนัง แต่หากคุณได้ติดตามบทความนี้ต่อไป จะได้รู้ว่า ไม่ใช่เรื่องยากเลย ที่ใครสักคนจะเจาะเข้ามาในระบบคุณ เอาข้อมูลไปขายให้คู่แข่งของคุณ หรือทำลายระบบงานที่เสียเงินจ้างมาวางระบบนับล้านบาท "มันไม่ยากอย่างที่ใคร ๆ คิด" ใช้ความพยายามเพียงเวลาว่างเพียง 3-4 ชั่วโมงหลังเลิกงานและวันหยุด นั่งรวบรวม และดาวน์โหลดโปรแกรมจากอินเทอร์เน็ต ทดลองโน่นทำนี่ไปเรื่อย ๆ จนหมดเวลา และวันหนึ่ง หลายสัปดาห์ต่อมาเขาก็พบช่องทางพบสิ่งที่ผู้บริหารระบบเคยคิดว่าเป็นเรื่องไร้สาระความประมาท เพราะไม่คาดคิดว่าจะมีใครมาสนใจระบบของเขากว่าจะรู้ก็สายเสียแล้ว

มีกลุ่มคนที่นิยมการแฮ็กอยู่มากมาย หนังสือที่ขายดีอันดับหนึ่งนานที่สุดของไทยเราเองก็เป็นหนังสือแฮ็ก หัวข้อกระทู้บนอินเทอร์เน็ต ที่ถามและได้รับความสนใจมากที่สุดก็เป็นเรื่องการแฮ็ก คีย์เวิร์ดที่ถูกใช้มากที่สุดของ Search engine ทุกแห่งก็คือคำว่า "แฮ็ก" เราเห็นการส่งไวรัสโทรจัน และขโมยข้อมูลกันบน อินเทอร์เน็ตทุกวันจนเป็นเรื่องปกติ มี เว็บไซท์และกลุ่มคนที่มีเวลาว่างมากพอที่จะศึกษาพวกนี้เป็นอาชีพ และเขียนโปรแกรมสำเร็จรูปเอามาแจกจ่ายให้กันฟรี ๆ พร้อมทั้งเอาข้อมูลวิธีการที่สำเร็จแล้ว มาเปิดเผย ช่องทางใหม่ ๆ ในการเจาะมีทุกวัน ผู้บริหารระบบต้องอัพเดตตัว Patch ตลอดเวลา คนเหล่านี้จะตรวจสอบเวอร์ชันของระบบคุณ แล้วตรวจสอบกับ เว็บไซท์ที่รายงานข้อบกพร่องของระบบ เปรียบเทียบรุ่นกัน แล้วก็ทราบได้ว่าระบบของคุณยังไม่ได้รับการปรับปรุง แล้วก็เจาะเข้าไปโดยที่คุณไม่รู้เลยว่าคุณกำลังถูกแฮ็ก หรือถูกแฮ็กไปแล้ว ซึ่งโดยมากแล้วแฮ็กเกอร์ฉลาดพอที่จะไม่สร้างความเสียหายทันทีกับระบบ แต่จะเก็บระบบไว้ใช้ประโยชน์ในระยะยาวมากกว่า



รูปที่ 1 เว็บไซท์ http://www.tlsecurity.net/Windows/cracker/ ตัวอย่างหนึ่งของที่มีข้อมูลเกี่ยวกับการแฮ็กและมีซอฟต์แวร์สำหรับแฮ็กให้ดาวน์โหลดกันฟรีๆ

เล่ห์เหลี่ยมกลลวงแฮกเกอร์

ภัยคนใกล้ตัว

ประมาณกันว่ากว่า 70 เปอร์เซ็นต์ของการแฮ็กเป็นฝีมือของคนใน (โดย American Society for Industrial Security) พวกเขาคุ้นเคย และเคยใช้งานระบบมาก่อน รู้ข้อมูลวงใน เข้าออกที่ทำงานง่าย อาจจะนั่งใกล้พนักงานด้วยกันที่มักจะแปะรหัสผ่านไว้ที่โต๊ะกันลืม หรือให้รหัสผ่านไว้เพื่อฝากให้ตรวจสอบข้อมูล สาเหตุที่คนในอยากจะแฮ็ก อาจจะมาจากความโกรธแค้น หรือไม่พอใจหน่วยงานตัวเอง พนักงานที่ถูกไล่ออก ถูกลดเงินเดือน ย้ายตำแหน่ง ตัดโบนัส ล้วนเป็นสาเหตุได้ทั้งนั้น อาจจะรู้ช่องทางที่จะเข้าไปเปลี่ยนแปลงข้อมูลคลังสินค้า การเงิน อาจจะปล่อยไวรัสเข้ามาทำลายระบบ ไวรัสพวกนี้หาง่าย ๆ ไปค้นตาม Search engine มีให้ดาวน์โหลดทั่วไป นอกจากนี้พวกเขายังมักจะได้รับการติดต่อจากบริษัทคู่แข่ง เสนอผลตอบแทนสูงเพื่อแลกกับข้อมูลภายในบริษัท

นอกจากพนักงานแล้วก็ได้แก่ บริษัทอื่นที่ร่วมงานกัน อาจจะเป็นตัวแทนจำหน่ายที่มีสิทธิในการเข้าระบบ หรืออาจจะเป็นผู้ที่เข้ามารับงานวางระบบ หรืองานโครงการชั่วคราวให้กับบริษัท อาจจะเป็นบริษัทที่ได้รับสิทธิพิเศษเพื่อแลกเปลี่ยนข้อมูลข่าวสารระหว่างกัน เช่น ระบบ EDI (เช่น กรมศุลกากรมีระบบ EDI ทำให้บริษัทนำเข้า ส่งออกสามารถใช้คอมพิวเตอร์ตรวจสอบพิกัด และอนุมัติสินค้าผ่านด่านได้ จากที่บริษัทเอง แทนที่จะต้องไปยื่นเอกสารที่มีขั้นตอนมากมาย)

การเปิดระบบสู่ภายนอก

หลาย ๆ บริษัทเริ่มให้พนักงาน สามารถเชื่อมต่อเข้าบริษัทเพื่อตรวจสอบ หรือทำรายการ มีคอมพิวเตอร์โน้ตบุ๊ค หรือเครื่องปาล์ม ทำให้พนักงานขายสามารถตรวจสอบยอดคงเหลือ ราคาล่าสุด พร้อมทำใบเสนอราคาได้ทันที ซึ่งมีประโยชน์มาก แต่ในทางตรงกันข้าม มันก็ลดระดับของความปลอดภัยต่อข้อมูลในองค์กรลง พนักงานเหล่านี้อาจไม่ให้ความสำคัญกับเรื่องของความปลอดภัยมากนัก อาจเอาเครื่องคอมพิวเตอร์ไปให้เพื่อนเล่น ให้ให้ร้านซ่อม อาจจะฝากของไว้กับโรงแรม หรืออาจจะปล่อยให้ใครมาเห็นรหัสผ่านได้ง่าย ๆ เครื่องคอมพิวเตอร์อาจหาย หรือถูกขโมยไปพร้อมกับข้อมูลสำคัญของบริษัท รายชื่อลูกค้า นอกจากนี้ การเปิดระบบสู่ภายนอกยังเปิดโอกาสให้ผู้ที่ไม่ประสงค์ดี สามารถเข้าสู่ระบบได้เป็นเวลานาน ๆ และควบคุมได้ยากกว่าขอบเขตของสำนักงาน

การเชื่อมต่อออกอินเทอร์เน็ต

อย่างที่ทราบกันดีว่า อินเทอร์เน็ตเป็นเครือข่ายที่ใหญ่ที่สุด หลายหน่วยงานเชื่อมโยงฐานข้อมูลในองค์กรสู่ภายนอกได้ ทำให้ลูกค้าสามารถส่งเพจเจอร์และ Short message service ผ่าน อินเทอร์เน็ต ตรวจสอบยอดเงิน ค่าใช้จ่าย ทำรายการโอนค้าหุ้น ตรวจสอบรายชื่อผู้ใช้โทรศัพท์ ซึ่งช่วยอำนวยความสะดวกสบาย แต่ขณะเดียวกัน ก็มีความเสี่ยงจากการที่ต้องเชื่อมต่อระบบเข้าสู่ อินเทอร์เน็ต แม้จะมีระบบป้องกันที่ดีก็ตาม ตัวอย่างเช่น ช่วงที่เพจเจอร์ให้บริการผ่านอินเทอร์เน็ต ใหม่ ๆ ก็เริ่มมีคนใช้ถ้อยคำหยาบคายส่งผ่านอินเทอร์เน็ต ซึ่งปกติข้อความเช่นว่าจะผ่านพนักงานรับโทรศัพท์ในระบบปกติไม่ได้ ต่อมาก็ถึงขั้นเขียนโปรแกรม CGI ส่งข้อความทีละเป็นร้อย กระจายกันทั่วไปหมด สุดท้ายบริษัทผู้ให้บริการก็ต้องเลือกใช้วิธีการให้เจ้าของแจ้งขอใช้บริการดังกล่าวก่อน จึงจะใช้ผ่านอินเทอร์เน็ตได้ คนก็เลิกใช้กันไปเพราะยุ่งยาก

การเข้าถึงระบบโดยตรง

ใครบางคนอาจเข้าถึงเครื่องคอมพิวเตอร์โดยตรง อาจถอดฝาเครื่อง ถอดแบตเตอรีของ เมนบอร์ด เพื่อยกเลิกรหัสผ่าน อาจจะทำ cloning ฮาร์ดดิสก์ หรือทำ laplink ข้อมูลออกไป มักจะเกิดกับองค์กรเล็ก ๆ ซึ่งไม่ค่อยให้ความสำคัญกับระบบความปลอดภัยนัก

วิธีวิศวกรรมสังคม (Social engineering)

เป็นวิธีการที่ไม่เน้นการใช้เทคโนโลยี อาจจะใช้วิธีการล่อลวงง่าย ๆ ในการได้มาซึ่งสิทธิ หรือรหัสผ่าน วิธีการก็คล้าย ๆ พวกนักเล่นกล หรือพวกแก๊งตกทองใช้ พวกที่ใช้เทคนิคล่อลวงโดยไม่ต้องใช้ความรู้ในการเจาะ หรือถอดรหัสเลย ข้อมูลอาจได้จากถังขยะ เศษของเอกสารที่ทิ้ง อาจจะใช้การพูด เจรจาเกลี้ยกล่อม โทรศัพท์เข้ามาแอบอ้าง แต่เชื่อเถอะว่า วิธีการทางสังคมถูกใช้มากที่สุด และเข้าถึงระบบได้ง่ายกว่าใช้เทคโนโลยีชั้นสูงเสียอีก

วิธีการเจาะระบบ

มีวิธีการเจาะเข้าสู่ระบบหลากหลายวิธีการ ในทางปฏิบัติแล้วมักจะใช้ร่วมกันตั้งแต่ 2-3 วิธีการขึ้นไป ขั้นตอนส่วนใหญ่จะมีเครื่องมือสำเร็จรูปให้ใช้กัน แต่บางขั้นตอนก็มีลักษณะเฉพาะซึ่งต้องเขียนโปรแกรมเฉพาะขั้นตอนนั้น ๆ ขึ้นมา มีคนไม่มากที่รู้วิธีการเจาะอย่างมืออาชีพ แต่เนื่องจากระบบความปลอดภัยบนคอมพิวเตอร์ในปัจจุบัน มีลักษณะสำเร็จรูปเน้นประโยชน์ใช้งานมากกว่าคำนึงถึงความปลอดภัย ระบบทั่ว ๆ ไปอย่าง Unix , NT, 2000 จึงถูกเจาะได้ไม่ยากนัก วิธีการที่ใช้กันพอจะแบ่งเป็นประเภทได้ดังนี้

การอ้างสิทธิเข้าสู่ระบบ

ผู้ที่จะเข้าสู่ระบบอาจจะเริ่มต้นเข้าสู่ระบบโดยอาศัยช่องทางทั่วไปที่เปิดให้ เช่น อาจเข้าถึงในนามของ Guest หรือ Anonymous (ซึ่งจะถูกจำกัดสิทธิเป็นอย่างมาก เพราะถือว่าเป็นคนนอก) เมื่อเข้าไปได้แล้ว ก็หาทางเพิ่มสิทธิให้กับตัวเอง ด้วยการหาไฟล์รหัสผ่าน หรืออาจหา Bug ของโปรแกรมที่ระบบนั้นมีอยู่ เช่นอาจจะใช้ช้อบกพร่องของโปรแกรม Mail เพื่อให้ตัวเองหลุดออกจาก Shell หรือหลุดจากการถูกจำกัดสิทธินั่นเอง บางทีก็หาไฟล์รหัสผ่านมาถอดรหัส โดยใช้โปรแกรมสำเร็จรูป เช่น โปรแกรม Cracker jack จากนั้นก็หาทางเพิ่มสิทธิของตัวเองเรื่อย ๆ เมื่อได้รับสิทธิเต็มที่ก็หาทางพรางตัวเองไม่ให้ถูกตรวจพบ โดยอาจเข้าไปลบบันทึก (Log files) ทำการเปิดช่องลับ ๆ (Backdoor) ให้ตัวเองสามารถเข้าสู่ระบบได้ในภายหลัง โดยที่เจ้าของระบบไม่ทราบ หรือบางทีก็ทำการเปลี่ยนรหัสผ่าน ยึดระบบเสียเลย (อย่างที่เห็น เว็บไซท์โดนยึดเปลี่ยนหน้าตากันบ่อย ๆ)

อีกวิธีหนึ่งก็โดยการชโมยรหัสผ่าน โดยอาจจะใช้โปรแกรม Keyboard capture ซึ่งจะดักจับการกดปุ่มของผู้ใช้ตลอดเวลา หรืออาจจะใช้โปรแกรมลวงหน้าจอ ซึ่งจะหลอกตัวเองเป็นหน้าจอของโปรแกรมที่ผู้ใช้ใช้งานบ่อย ๆ ให้ผู้ใช้ใส่รหัสผ่านเข้าไป หรือบางทีอาจจะได้รับรหัสผ่านนั้น ๆ จากการแกะรหัสผ่าน เช่น ใน Win9x สามารถถูกแกะได้โดยง่ายโดยใช้โปรแกรม pwlview.exe เมื่อได้รหัสผ่านมาแล้ว ก็มักจะถูกนำไปใช้อย่างต่อเนื่อง บนสมมุติฐานว่า คนส่วนใหญ่ มักจะมีรหัสผ่านในใจไม่กี่ชุด และมักจะใช้รหัสผ่านเดียวกันนี้กับหลาย ๆ ที่ ทำให้เมื่อเจาะเข้าสู่ระบบใดได้แล้ว ก็มักจะเจาะระบบอื่น ๆ ของผู้ใช้รายนั้น ๆ ได้ไม่ยาก เช่นอาจได้รหัสผ่านของ Windows98 มา แต่ผู้ใช้คนนั้นใช้รหัสผ่านเดียวกันนี้กับ เว็บไซท์หรือ E-mail ด้วย

อย่ามั่นใจในระบบความปลอดภัยตามที่โฆษณามาก เพราะแม้จะซื้อระบบที่ยอดเยี่ยมมา เป็นตัวเดียวกับที่ใช้ที่อื่นมาแล้วอย่างได้ผล แต่การตั้งค่าระบบที่ไม่เหมือนกัน ย่อมทำให้การป้องกันที่ดีแตกต่างกันไปด้วย ผู้เขียนเคยเห็น Admin ทั้งหลาย ติดตั้ง Firewall แล้วยืดอกอย่างมั่นใจว่าระบบที่ตัวเองวางปลอดภัย แท้ที่จริงเพียงแค่ติดตั้งโปรแกรมเข้าไป แล้วใช้ค่า Default ที่โปรแกรมนั้นให้มา พึงระลึกไว้ว่า ค่า Default นั้น ผู้ผลิตให้มาเพื่ออำนวยความสะดวกในการติดตั้ง และใช้งานมากกว่า หลายส่วนของระบบอาจถูกปิดหรือตั้งในระดับปลอดภัยต่ำไว้ในเบื้องต้น และให้ผู้ใช้เป็นคนกำหนดเพิ่มระดับการป้องกันเอาเอง

วิธีการเข้าสู่ระบบนั้น อาจเข้าจากภายนอกองค์กรก็ได้ เช่น กรณีที่รู้ว่ามีการต่อโมเด็ม เพื่อรับการเชื่อมต่อจากภายนอกได้ ผู้ประสงค์ร้าย อาจจะใช้คอมพิวเตอร์โน้ตบุ๊ค พร้อมใช้โปรแกรมหมุนโทรศัพท์ที่เรียกว่า War dialer โปรแกรมนี้จะทำการหมุนโทรศัพท์ไปเรื่อย ๆ แล้วบันทึกผลลัพธ์ของการหมุนเอาไว้ ว่ามีการตอบรับอย่างไร โดยการเดาเลข 3 ตัวหน้าของเขตโทรศัพท์นั้น ๆ ส่วนอีก 10000 ตัวที่เหลือก็อาจไปพ่วงกับโทรศัพท์ตึกไหนสักแห่ง หรือตู้สาธารณะ คืนเดียวก็เสร็จ ได้รายการเบอร์โทรตามที่ต้องการ

การป้อนข้อมูลที่ไม่เหมาะสมสู่ระบบ

บนระบบที่ต้องมีการรับข้อมูลเข้า อาจจะเป็นโปรแกรมที่เชื่อมโยงเข้ากับฐาน

ข้อมูล โปรแกรมนั้น ๆ อาจเป็น Form ที่อยู่บน อินเทอร์เน็ต เพื่อให้ลงทะเบียน หรือสืบค้นข้อมูล หากในขั้นตอนการออกแบบโปรแกรม ไม่ได้มีการจำกัดปริมาณข้อมูลรับเข้า ก็อาจถูกโจมตีโดยการใส่ข้อมูลที่ผิด ๆ หรือมีปริมาณมากเกินกว่าโปรแกรมจะรับไหว ซึ่งอาจจะส่งผลให้ระบบ Hang หรือทำงานผิดปกติ อาจคายข้อมูลบางอย่าง หรือเปิดช่องให้เจาะเข้าสู่ระบบได้

โปรแกรมใช้งานบางโปรแกรม อาจเปิดโอกาสให้ Append ข้อมูลโดยใช้คำสั่ง SQL ซึ่งสะดวกใช้ แต่ในบางกรณี อาจมีคนเขียนโปรแกรมขึ้นมาเอง เรียกใช้คำสั่ง SQL โดยตรง ไม่ผ่าน Form ที่เรากำหนด ทำให้สามารถเข้าถึงข้อมูลได้มากกว่า บางครั้งอาจเข้าถึงฐานข้อมูลระดับลึก เปลี่ยนแปลง เพิ่ม ลบ ผู้ใช้ ในระบบได้

อาศัยความเชื่อถือ หรือลวง

ระบบเครือข่ายมักจะมีการกระจายอำนาจการบริหารระบบให้กับระบบอื่น หรือสร้างความสัมพันธ์กันระหว่างระบบ เพื่อให้สามารถแลกเปลี่ยนข้อมูลข่าวสารกันได้ ระบบอาจถูกติดตั้งและตรวจสอบมาอย่างดีในที่หนึ่ง แต่เครือข่ายที่กระจายอำนาจให้ไป อาจมีช่องโหว่ เปิดโอกาสให้มีการเจาะผ่านระบบอื่นที่เราไว้วางใจเข้ามาได้ (เคยมีกรณีที่ องค์การอวกาศของสหรัฐฯ หรือ นาซ่า ถูกเจาะระบบ โดยแฮ็กเกอร์ เจาะผ่านสนามบินเล็ก ๆ แห่งหนึ่งได้ แล้วใช้สิทธิของสนามบินนั้น ๆ ที่ทางนาซ่าไว้วางใจ เข้าสู่ระบบ)

บางวิธีจะใช้การส่งข้อมูลลวงเข้าไปในระบบเครือข่าย โดยข้อมูลหลอกเข้าไปสื่อสารกับระบบที่ต้องการ ทำให้คอมพิวเตอร์ปลายทางเข้าใจผิดว่ามาจากเครื่องที่ถูกต้อง หรือบางทีระหว่างที่คอมพิวเตอร์สองตัวกำลังสื่อสารกันอยู่ ก็โจมตีคอมพิวเตอร์เครื่องหนึ่งให้หยุดทำงานเสีย แล้วสวมรอยเป็นคอมพิวเตอร์เครื่องนั้น ๆ เข้าไปสื่อสารแทน บางทีก็ใช้วิธีวางยาเบื่อ ส่งข้อมูลบางอย่างเข้าไปทำให้ระบบไม่สามารถประมวลผลได้ เพื่อให้ระบบคายข้อมูลสำคัญบางอย่างออกมา

ดักจับข้อมูล

มีโปรแกรมบางประเภท สามารถดักดูข้อมูลได้ โปรแกรมพวกนี้หา ดาวน์โหลดจาก อินเทอร์เน็ต ได้ง่าย เรียกว่า Sniffers โดยอาศัยหลักการที่ว่า มีการส่งข้อมูลผ่านสาย LAN ตามปกติอยู่ตลอดเวลา ปกติแล้วเครื่องที่กำหนดจะรับข้อมูลมาสู่ผู้ใช้ แต่เมื่อใช้โปรแกรมนี้ จะมองเห็นข้อมูลทั้งหมดที่วิ่งอยู่บนเครือข่าย ไม่ว่าจะส่งถึงใคร หลาย ๆ ส่วนของข้อมูลเป็นข้อความธรรมดาที่ไม่ได้เข้ารหัส สามารถเก็บบันทึกเป็นไฟล์ข้อความ และอ่านออกมาตรง ๆ หรือใช้โปรแกรมกลั่นกรองข้อมูลเฉพาะที่ต้องการเช่น รหัสผ่าน ออกมาอีกที

ใช้โปรแกรมหรือบริการ

ลูกเล่นและบริการต่าง ๆ ที่ผู้บริหารระบบนำมาใส่มักเปิดช่องโหว่เพิ่มขึ้นให้กับระบบเสมอ รวมทั้ง Service และ Protocol ที่เรียกใช้ก็เปิดช่องทาง ผู้บริหารอาจจะต้องเลือก ที่จะยอมให้ระบบมีรูโหว่บ้าง เพื่อแลกกับการได้ใช้งานแอพพิเคชันต่าง ๆ แม้แต่โปรแกรม Utilities ที่ติดตั้งมาพร้อมกับ OS อย่างเช่น FTP , Telnet ล้วนแต่เป็นเครื่องมือของระบบเอง ที่มีอานุภาพสูง นอกจากนี้ Service บางตัว เช่น DNS , IIS ล้วนมีช่องโหว่เช่นกัน บางทีก็ใช้ภาษา VB Script หรือ JavaScript ในการเจาะเข้าไป นอกจากนี้ยังมีวิธีการอื่น ๆ อีกมาก เช่น การขโมย Port , การโจมตีให้บริการระบบรักษาความปลอดภัยถูกทำลาย (Denial of Service) โดยใช้โปรแกรม หรือข้อมูลทำให้ระบบความปลอดภัยเช่น Firewall หยุดทำงาน

ไวรัส หนอน ม้าโทรจัน

ไวรัสอาจถูกส่งมายังเครื่องคุณได้เช่นกัน พวก E-mail แปลก ๆ ไม่ระบุชื่อที่อยู่ผู้ส่ง แนบไฟล์แปลก ๆ มาด้วย ล้วนต้องสงสัยด้วยกันทั้งนั้น ผู้เขียนเองได้รับ E-mail ประเภทนี้เข้ามาทุกวัน ไฟล์โปรแกรมที่แนบมาอาจมีข้อความเชิญชวนให้สนใจ เมื่อเราเปิดหรือเรียกใช้งาน มันก็อาจปล่อยไวรัสหรืออาจติดตั้งโทรจันลงบนเครื่องของเรา โทรจันก็คือโปรแกรมประเภทหนึ่ง ที่ฝังตัวอยู่ในเครื่องเรา เปิดช่องโหว่ให้ฝ่ายตรงข้ามเข้ามาควบคุม หรือใช้ทรัพยากรบนเครื่องเราได้โดยเราไม่รู้ตัว นอกจากนี้ ยังมีหนอน (Worm) ไม่เหมือนกับไวรัส หนอนจะมีความสามารถ ฉลาดกว่า ขนาดใหญ่กว่า มันทำงานได้ด้วยตัวเอง เสาะหาช่องทางผ่านระบบไปเรื่อย ๆ และสามารถทำงานอยู่ตลอดเวลาโดยไม่จำเป็นต้องมีใครเรียกใช้ไฟล์ก่อนเหมือนไวรัส โปรแกรมบางตัวเมื่อติดตั้งเข้ามาในระบบเรา ก็จะเปิดช่องโหว่ไว้สำหรับผู้ไม่หวังดีเข้ามาได้

มาตรการการรักษาความปลอดภัย

เราได้กล่าวถึงรูปแบบต่าง ๆ ของการรุกรานที่เป็นไปได้ คำถามคือ เราจะป้องกันได้อย่างไร?

เก็บข้อมูลภายใน

ปราการด่านป้องกันเปรียบเสมือนบ้านของคุณ มีสิ่งที่คุณจำเป็นต้องรู้เกี่ยวกับบ้าน มีประตูกี่บาน ทรัพย์สินมีค่าหยิบฉวยง่ายมีอะไรบ้าง มีกลอน และสัญญาณเตือนภัยอย่างไร ? ไม่แตกต่างกันเลยกับระบบความปลอดภัยบนคอมพิวเตอร์ สิ่งที่คุณจำเป็นต้องรู้ได้แก่

- มีข้อมูลอะไรบ้างที่มีค่า เก็บไว้ที่ไหน และจะเกิดความเสียหายอย่างไรแก่คุณบ้าง หากถูกขโมยหรือทำลาย
- ระบบของคุณมีจุดเชื่อมต่ออย่างไร ? ใครบ้างที่มีสิทธิเข้าใช้ระบบ มีช่องทางไหนบ้างที่จะสามารถเข้าถึงข้อมูลได้ เช่นผ่านอินเทอร์เน็ต , LAN , Dial , Laplink และแม้แต่การ load ผ่าน ฮาร์ดดิสก์โดยตรง
- ประวัติการทำงานของบุคลากรภายใน และบุคคลากรที่ต้องเข้ามาเกี่ยวข้องกับระบบ

วางแผนกำหนดมาตรการป้องกัน

- นำข้อมูลที่ได้มาวิเคราะห์ หามาตรการป้องกัน โดยกำหนดแยกแยะข้อมูล สถานที่เก็บให้เป็นระเบียบเรียบร้อย

กำหนดระดับความสำคัญของข้อมูล และสิทธิการเข้าถึงเสียใหม่

- เลือก และติดตั้งระบบรักษาความปลอดภัยให้กับคอมพิวเตอร์ เช่น Firewall เข้ารหัสข้อมูลเสียใหม่ ระบบตรวจจับและดูความเคลื่อนไหวในการใช้งานระบบของผู้ใช้ รวมทั้งการที่เอา เซิร์ฟเวอร์ เก็บในตู้และห้องที่เป็นสัดส่วน เพื่อป้องกันการเข้าถึงบัญชีผู้ใช้โดยตรงจาก ฮาร์ดดิสก์
- หาบุคลากรมารับผิดชอบ ตามนโยบายความปลอดภัยที่วางไว้ ชี้ให้เห็นถึงความสำคัญของการรักษาความปลอดภัย พร้อมทั้งออกระเบียบ มาตรการลงโทษ
- แยกประเภทบุคลากรออกจากกัน พนักงานประจำ ลูกจ้างชั่วคราว บุคคลภายนอก และรับจ้าง ให้ติดบัตรเพื่อแสดงตัวทุกครั้งในที่ทำงาน
- จัดประชุมบุคลากร ชี้แจงนโยบาย มาตรการ ทำเอกสารรายละเอียดการใช้งานระบบอย่างถูกวิธี

การควบคุมการใช้งานระบบ

ควบคุมการเข้าถึงและใช้งานระบบ

เราสามารถควบคุมการเข้าสู่ระบบได้มีหลายวิธีการที่นำมาใช้กัน ส่วนมากแล้วเราจะเห็นการเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านเป็นเครื่องปกติ แต่หากเป็นลักษณะงานที่ต้องการความปลอดภัยสูงขึ้นแล้ว ควรพิจารณาวิธีการอื่น ๆ ร่วมด้วย การใช้มากกว่าหนึ่งวิธีการร่วมกัน จะทำให้ระบบปลอดภัยมากขึ้นทวีคูณ สิ่งที่ควรคำนึงถึงเพื่อตัดสินใจเรื่องวิธีเข้าสู่ระบบ คือ

- สิ่งที่คุณมี เช่น กุญแจ หรือสมาร์ตการ์ด
- สิ่งที่คุณรู้ เช่น ชื่อผู้ใช้ สถานที่เก็บรหัสผ่าน
- สิ่งที่คุณมี เช่น ลายนิ้วมือ สแกนม่านตา

เมื่อควบคุมการเข้าสู่ระบบได้แล้ว สิ่งที่ต้องพิจารณาต่อไปก็คือ จะต้องควบคุมข้อมูลในระบบสำหรับคนที่เข้าระบบได้แล้วโดยการ กำหนดการป้องกัน และสิทธิการเข้าถึงทรัพยากรแต่ละคน มิฉะนั้นคนหนึ่ง ๆ จะสามารถเข้าถึงข้อมูลในทุก ๆ ที่ อาจเผลอไปลบไฟล์ของคนอื่นเข้าก็ได้

ผู้เขียนเห็นหลาย ๆ สำนักงานใช้ Windows9x ในการทำงาน แบ่งใช้ไฟล์และเครื่องพิมพ์ กัน ซึ่งเหมาะสำหรับสำนักงานขนาดเล็ก มีคนเพียงไม่กี่คน ดูแลกันเองแบบง่าย ๆ แต่หากสำนักงานใหญ่ขึ้น มีบุคลากรมากขึ้น ควรพิจารณาระบบเครือข่ายแบบ Client/เซิร์ฟเวอร์ เพราะจะให้ความปลอดภัย รวมทั้งความสามารถในการทำงานอื่น ๆ อีกมากมายมหาศาล

สำหรับระบบที่เข้มงวดมากขึ้น

ไม่ใช่ว่าการป้องกันการเข้าสู่ระบบทำได้ดีแล้ว จะทำให้ปลอดภัย บางที่ผู้ที่จะขโมยข้อมูล อาจไม่จำเป็นต้องมีสิทธิการเข้าถึงมาก่อนเลยก็ได้ โปรแกรมบางตัวที่ใช้กันทั่ว ๆ ไปบนระบบเครือข่าย เช่น FTP Telnet และโปรแกรมอื่น ๆ ที่ใช้โปรโตคอลที่ไม่ได้เข้ารหัส เช่น TCP/IP, UDP พวกนี้จำส่งรหัส และชื่อผู้ใช้เป็นข้อความธรรมดาผ่านสายสัญญาน ซึ่งผู้ที่ต้องการจะเจาะข้อมูลสามารถใช้โปรแกรม หรือเครื่องมือ Sniffer ดูข้อมูลเหล่านั้นได้ ตัวอย่างที่รูปที่ 2

จะเห็นได้ว่าข้อมูลต่าง ๆ ที่วิ่งอยู่บนสายนั้น ไม่ได้ปลอดภัยเลย ผู้เขียนยังสังเกตว่า ตู้ ATM ที่วางอยู่ตามห้างนั้น เชื่อมต่อสัญญานผ่านโมเด็มรุ่นเก่า มีโอกาสที่จะถูกดักเอาข้อมูลและรหัส ATM ได้เหมือนกัน วิธีป้องกันก็เช่น เลือกใช้ซอฟต์แวร์ที่มีความสามารถในการเข้ารหัสข้อมูลภายในสายสัญญาณได้ เช่น Windows NT ถ้าเป็นระบบอย่าง Windows 2000 จะมีโปรโตคอล LDAP ซึ่งปลอดภัยกว่า TCP/IP หรือ Netbuei

นอกจากนี้ ยังมีวิธีการอื่น ๆ อีกเช่น การกำหนดให้เซิร์ฟเวอร์เราตรวจสอบได้ด้วยว่ามีการเชื่อมต่อมาจากโทรศัพท์เบอร์ไหน ผู้เขียนเห็นศูนย์ อินเทอร์เน็ต บางแห่ง (อินเทอร์เน็ต cool pack ของ E-Znet) เอาตรงนี้เข้ามาใช้ หากไม่ได้หมุนอินเทอร์เน็ต เข้ามากจากเบอร์โทรศัพท์ที่กำหนดแล้ว จะ Logon ไม่ได้ ซึ่งโทรศัพท์ในเขตนั้น ๆ ต้องแสดงเบอร์ได้ รวมทั้งซอฟต์แวร์ของเราต้องสนับสนุนด้วย

กำหนดข้อบังคับเรื่องรหัสผ่าน

ควรกำหนดกติกาข้อบังคับเรื่องรหัสผ่านให้ดี ผู้ใช้ส่วนใหญ่ แม้กระทั่งระดับผู้บริหาร หรือผู้จัดการ นิยมใช้คำง่าย ๆ ใกล้ตัว อาจจะเป็นชื่อภรรยาที่รัก มาตั้งเป็นรหัสผ่าน ที่พบมากที่สุดคือการแปะรหัสผ่านที่โต๊ะทำงาน หรือหน้าจอมอนิเตอร์ แม้รหัสผ่านนั้นอาจจะเป็นของคนที่ไม่สำคัญ และมีสิทธิในการเข้าระบบน้อย แต่ก็ทำให้เกิดช่องทางเข้าสู่ระบบ ผู้บุกรุกอาจจะใช้สิทธิน้อย ๆ นี้เข้าไป จากนั้นก็รัน Exploit เพื่อยกเลิกระบบความปลอดภัยบางอย่าง เพิ่มสิทธิให้ตัวเองสูงขึ้น และอีกสารพัดแต่จะสรรหากันมา ซอฟต์แวร์ระบบเครือข่ายหลายระบบสนับสนุนข้อกำหนดในการตั้งรหัสผ่าน รวมถึงสามารถกำหนดอายุของรหัสผ่าน บังคับให้ผู้ใช้เปลี่ยนตามเวลาที่กำหนดได้ และยังสามารถล็อกการทำงานของรหัสผ่านนั้น ๆ กรณีมีการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนด

อีกวิธีที่จะขโมยรหัสผ่านได้ก็คือ การใช้โปรแกรม Keyboard capture โปรแกรม

```
0000:  03 00 00 00 00 01 00 E0 29 53 51 B5 00 B9 F0 F0  ........)SQ.....
0010:  03 2C 00 FF EF 08 00 00 00 00 00 00 00 49 54 53  .,...........ITS
0020:  51 55 41 52 45 20 20 20 20 20 20 20 1E 53 43 4F  QUARE       .SCO
0030:  52 50 49 4F 4E 20 20 20 20 20 20 20 00 FF 53 4D  RPION       ..SM
0040:  42 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00  B%..............
0050:  00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00  ................
0060:  34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  4...............
0070:  00 00 00 00 34 00 56 00 03 00 01 00 01 00 02 00  ....4.V.........
0080:  45 00 5C 4D 41 49 4C 53 4C 4F 54 5C 42 52 4F 57  E.\MAILSLOT\BROW
0090:  53 45 00 0F 06 C0 D4 01 00 53 43 4F 52 50 49 4F  SE.......SCORPIO
00A0:  4E 00 00 00 00 00 00 00 00 00 04 00 03 20 45 00  N............ E.
00B0:  04 55 AA 4E 41 54 54 41 50 4F 4E 47 20 53 41 4D  .U.NATTAPONG SAM
00C0:  41 54 49 57 41 54 00                             ATIWAT.
```

รูปที่ 2 การแสดงถึงข้อมูลที่ส่งผ่าน LAN โดยที่ผู้เขียนใช้โปรแกรมดักจับข้อมูล จะเห็นว่าข้อมูลที่ส่งนั้นมีข้อความที่ระบุชื่อผู้ใช้และข้อมูลอื่น ๆ วิ่งอยู่ด้วย

รูปที่ 3 เมื่อผู้เขียนดักจับข้อมูลผ่านสายโทรศัพท์โมเด็มที่เชื่อมต่อเข้าอินเทอร์เน็ต จะมีข้อมูลส่วนหนึ่งที่แสดงชื่อและรหัสผ่านเข้าสู่ อินเทอร์เน็ต

นี้ จะซ่อนตัวอยู่เงียบ ๆ คอยดักจับข้อความที่ผู้ใช้พิมพ์ แล้วบันทึกเป็นไฟล์ซ่อนไว้ บางทีก็เอาที่บันทึกไว้ส่งออกทาง E-mail ไปยังผู้ที่ลักลอบ เรียกว่าเสิร์ฟถึงโต๊ะอาหารเลย ตรงนี้ป้องกันได้ดีที่สุดก็โดยการป้องกันไม่ให้คนอื่นเข้ามายุ่งกับเครื่องของเรา อย่างไรก็ตาม ผู้บุกรุกอาจจะใช้วิธีส่ง E-mail มาหาเรา พร้อมข้อความท้าทาย หรือให้สงสัย อาจจะบอกว่าเป็นโปรแกรมเด็ดอะไรทำนองนั้น พวกนี้ส่วนมากไม่ระบุชื่อที่อยู่ของผู้ส่ง พอเราเปิดโปรแกรมนั้นดู อาจเป็นโปรแกรมที่น่าสนใจตามที่ต้องการ พร้อมด้วยติดตั้งโปรแกรมดักข้อมูลลงในเครื่องเราเสร็จสรรพ อย่าโทษหรือโกรธใครเลย คุณเองเป็นคนติดตั้ง ใช่ไหมครับ

สำหรับตัวผู้บริหารระบบเอง ก็ควรระมัดระวัง ไม่ให้ใครเข้าถึงไฟล์ที่เกี่ยวข้องกับระบบความปลอดภัย ตรงนี้แตกต่างไปแล้วแต่ระบบที่ใช้ Unix ก็แบบหนึ่ง NT ก็แบบหนึ่ง จงศึกษาเพื่อใช้งานระบบนั้น ๆ อย่างเข้าใจ เพราะแม้ไฟล์เหล่านั้น แม้จะไม่สามารถเปิดเพื่ออ่านรหัสผ่านได้โดยตรง แต่ก็สามารถใช้โปรแกรม Dictionary ถอดรหัสออกมาได้

การป้องกันการวางยาระบบ

ระบบอาจถูกใครแอบวางยา โดยการป้อนข้อมูลบางอย่างเข้ามา แม้ระบบจะถูกตั้งค่ามาปลอดภัยดีแล้ว ในระดับของผู้ใช้ แต่ระบบก็ยังคงต้องการการติดต่อสื่อสารในระดับพื้นฐานบางตัว หรือบางทีจำเป็นต้องเปิดช่องสำหรับรับลูกค้า หรือเปิดช่องทางสำหรับโปรแกรมใช้งาน ซึ่งช่องทางเหล่านี้อาจถูกใช้สำหรับโจมตีด้วยวิธีการวางยาได้ ตัวอย่างของการวางยาได้แก่

- บนอินเทอร์เน็ตเราใช้เว็บเพจสำหรับรับข้อมูล input จากผู้ใช้ตัวแบบฟอร์มรับข้อมูลสามารถถูกเปิดอ่านภาษา HTML ได้โดยง่าย และเปิดเผยที่ตั้งของไฟล์ CGI หรืออาจมีการเรียกใช้คำสั่ง SQL โดยตรงในฟอร์ม เหล่านี้อันตราย เพราะอาจมีการเขียนโปรแกรมเจาะฐานข้อมูล หรือส่งข้อมูลจำนวนมากเข้าไปเพื่อหยุดระบบได้ วิธีป้องกันก็คือ เลือก หรือเขียนโปรแกรมที่มีการรันในฝั่ง เซิร์ฟเวอร์ และการรับข้อมูลทุกชนิด ให้เขียนโปรแกรมตรวจสอบ และจำกัดขนาดของข้อมูลที่รับเข้าไปเสมอ
- โปรแกรมมีการเรียกใช้ฟังก์ชันของ Windows เช่น ฟังก์ชัน API ผู้บุกรุกอาจอาศัยช่องนี้สวมรอยเข้าไปอ่านเขียนโดยตรงผ่านฟังก์ชัน หรืออาจตั้งใจรันคำสั่งที่ผิดพลาดทำให้โปรแกรมป้องกัน หรือ Service หยุดทำงาน หรือทำงานผิดปกติ ซึ่งคุณสามารถป้องกันได้โดยไม่อนุญาตให้เอาโปรแกรมจากภายนอกมารันในระบบโดยไม่ได้รับอนุญาต (ดูจะเป็นไปได้ยากในทางปฏิบัติ กฎระเบียบมากไป ระบบงานก็จะเสียความยืดหยุ่น ยุ่งยาก ลดประสิทธิภาพงานเสียอีก จะตั้งระบบความปลอดภัยเข้มขนาดไหน ดูความเหมาะสมด้วยนะครับ)

แต่ละโปรแกรมที่เราใช้งานอยู่ ต่างก็มีข้อบกพร่องทุกตัว ข้อบกพร่องนี้จะถูกค้นพบออกมาเรื่อย ๆ และเผยแพร่กันอย่างรวดเร็วบน อินเทอร์เน็ต คุณจึงควรตรวจสอบกับผู้ผลิตโปรแกรมนั้น ๆ ตัวอย่างเช่น Windows NT /2000 ก็จะมี Patch ออกมาเรื่อย ๆ เช่น Service pack ต่าง ๆ ก็คือตัวแก้ Bug ที่ออกตามมาทีหลังนั่นเอง เพื่อปรับปรุงระบบ และปิดช่องโหว่ ส่วนมากจะให้เข้าไปดาวน์โหลดกันได้ฟรีที่เว็บไซท์ของผู้ผลิตรายนั้น ๆ เป็นการสนับสนุนหลังการขาย ผู้บุกรุกสามารถใช้โปรแกรมเพื่อตรวจสอบรุ่นของระบบเราได้ หากเขารู้รุ่นแล้ว เขาจะใช้เว็บไซท์เดียวกันของผู้ผลิตนั่นแหละเป็นแหล่งข้อมูลว่าก่อนการปรับปรุงมีข้อบกพร่องอะไรบ้าง ถ้าเขารู้ว่าคุณยังไม่อัพเดตคุณก็เสร็จ

หากมีการส่งข้อมูลกันเองเป็นประจำระหว่างสาขา หรือข้อมูลที่ใช้ภายใน ก็ควรตั้งค่าทั้ง 2 ฝั่งให้มีการเข้ารหัสข้อมูลที่ส่งเสมอ โปรโตคอลที่เข้ารหัสก็มีหลายรูปแบบมาก เช่น PGP, SSL , HTTPS , IPSec ซึ่งในรายละเอียดคงจะได้กล่าวถึงในบทต่อ ๆ ไป

ป้องกันไวรัส หนอนโทรจัน

วิธีที่ง่ายที่สุด และใช้กันอยู่ทั่วไป ก็คือการใช้โปรแกรมป้องกันและฆ่าไวรัส ซึ่งมีทั้งแบบที่เป็น ฮาร์ดแวร์และ ซอฟต์แวร์ แบบที่เป็น ฮาร์ดแวร์ปัจจุบันไม่ค่อยนิยมใช้กันแล้ว มีคำโฆษณาว่าดีกว่าแบบซอฟต์แวร์แต่จริงๆ แล้ว ก็เหมือน ๆ กัน ขึ้นอยู่กับคุณภาพงานวิจัย และข้อมูลไวรัสของผู้ผลิตรายนั้น ๆ มากกว่า แบบที่เป็นซอฟต์แวร์ก็มีหลากหลาย ส่วนมากจะให้ดาวน์โหลด ใช้กันฟรี ๆ ยกเว้นจะเป็นรุ่นสำหรับระบบเครือข่าย หรือรุ่นที่ความสามารถมากขึ้น แต่ขอเตือนว่า เมื่อติดตั้งไปแล้วก็อย่าไว้วางใจมากนัก เพราะไวรัสมีออกใหม่วันละหลายตัวทุกวัน โปรแกรมฆ่าไวรัส ไม่สามารถตรวจหาไวรัสชนิดที่ใหม่กว่าตัวมันได้ สิ่งที่ต้องคำนึงถึง เพื่อเตือนใจเสมอ คือ

- โปรแกรมฆ่าไวรัสไม่สามารถฆ่าไวรัสได้ทุกตัว และแต่ละยี่ห้อ ก็สามารถฆ่าไวรัสได้ต่างชนิดกันไป อาจต้องใช้มากกว่า 1 ยี่ห้อร่วมกัน
- ต้องอัพเดตข้อมูลไวรัสเสมอ ปกติแล้วโปรแกรมฆ่าไวรัสจะมี Live update หรืออาจจะมีเมนูสำหรับให้อัพเดตไวรัส

ใหม่ ๆ อยู่ในตัวโปรแกรม

- หากไวรัสติดเข้าไปในระบบปฏิบัติการแล้ว ไวรัสบางตัวมีความสามารถในการหลอกโปรแกรมฆ่าไวรัสได้ หรือแม้แต่ทำให้โปรแกรมฆ่าไวรัสหยุดทำงานไปเลย ตรงนี้อาจต้องเอาฮาร์ดดิสก์ของเครื่องที่ย่ำแย่แล้ว ไปใส่ในเครื่องอื่นที่มีโปรแกรมฆ่าไวรัสอยู่ด้วยความระมัดระวัง แล้วใช้เครื่องอื่นฆ่าให้มาตรการที่ดีกว่าการแก้ไขก็คือการป้องกัน ดังนั้น
- ควรติดตั้งโปรแกรมฆ่าไวรัสทุกเครื่องก่อน ไม่ใช่ไปติดตั้งทีหลังใช้เครื่องไปแล้ว จะให้ผลที่ดีกว่า เพราะโปรแกรมฆ่าไวรัสมีการเก็บค่าไฟล์ หากติดตั้งก่อน ก็พอจะช่วยป้องกันไวรัสชนิดใหม่ที่ยังไม่มีข้อมูลได้บ้าง
- การกำหนดสิทธิให้ผู้ใช้อ่านได้อย่างเดียว จะทำให้พื้นที่นั้น ๆ ไม่ติดไวรัส (แต่ก็อาจจะติดได้ ในตอนที่เราใช้รหัสผ่านที่อ่านเขียนได้เข้าไปดู)
- สำรองข้อมูลอย่างน้อย 3 ชุดเสมอ เผื่อเสียหายแก้ไม่ไหวจริงๆ จะได้ดึงข้อมูลชุดเก่ามาแทนได้
- ยกเลิก Floppy disk , CD-ROM ในเครื่องที่ไม่จำเป็นต้องมี และกำหนดห้ามเอาแผ่นจากภายนอกเข้ามาเล่นโดยไม่ได้รับอนุญาต
- ไม่รับไฟล์แปลกหน้า ไม่ว่าจะมาจากดิสก์เกตต์ หรือ E-mail หากจำเป็นจริงๆ ก็ให้ใช้โปรแกรมฆ่าไวรัสตรวจสอบก่อนเสมอเวลาที่ไวรัสแพร่ไปบนระบบเครือข่าย มักจะเป็นเรื่องที่ปวดหัวมาก บางทีมันจะกระจายไปอย่างรวดเร็วนับร้อย ๆ เครื่องในเวลาไม่กี่นาที เราตามฆ่ามันไม่หมด ฆ่าที่เครื่องนี้ มันก็วิ่งไปเครื่องอื่น ส่วนเครื่องที่เราล้างใหม่แล้ว ไม่กี่นาทีก็ติดอีก ทำให้เราต้องออกจากระบบเครือข่ายก่อน แล้วค่อยฆ่าแยกกันโดยไม่เชื่อมต่อ อย่างไรก็ตาม โปรแกรมฆ่าไวรัส เช่น Norton antivirus coporate edition มีความสามารถตามไปจัดการเครื่องอื่น ๆ ในเครือข่ายได้อย่างมีประสิทธิภาพ

ระวังการเข้าถึงเครื่องโดยตรง

การเข้าถึงผ่านระบบ Remote เป็นการเข้าถึงที่ง่ายที่สุด และปลอดภัยกับตัวผู้บุกรุกที่สุด แต่หากเข้าถึง Node ใดของระบบเครือข่ายภายในได้ ถือว่าโอกาสสูงที่จะเจาะ และหากเข้าถึงเครื่อง เซิร์ฟเวอร์ได้แล้วล่ะก็ ไม่เหลือละครับครับ เพราะการเข้าถึงเครื่องโดยตรงได้นั้น จะทำให้เข้าถึงไฟล์ที่ปกติถูกป้องกันผ่านเครือข่าย แม้จะเข้ารหัสไว้ แต่ก็สามารถถอดได้ แทบไม่มีข้อจำกัดแล้ว หากปล่อยให้เข้าถึงโดยตรงได้ เราต้องป้องกันโดย

- ตั้งรหัสผ่านระดับ CMOS ไว้ จะเป็นการป้องกันด่านแรก อย่างน้อยก็ให้เข้าไม่ถึงดิสก์ อย่างไรก็ตาม ก็ไม่ยากเลยที่จะ Reset หรือถอดแบตเตอรีของ เมนบอร์ด เพื่อปลดรหัสผ่าน
- ใช้โปรแกรมป้องกัน ฮาร์ดดิสก์หรือโปรแกรมรหัสผ่านก่อนเข้าถึง ฮาร์ดดิสก์
- เข้ารหัสข้อมูลทั้งหมดบน ฮาร์ดดิสก์ วิธีนี้ดีมาก แต่ก็ทำให้เครื่องช้าลงมากเช่นกัน
- ยกเลิก Floppy disk , CD , พอร์ต และ อุปกรณ์อื่น ๆ ที่ไม่ได้ใช้เดี๋ยวนั้นออกเสีย ใช้เมื่อไรค่อยเสียบเข้าไป
- วางเครื่องไว้ในสถานที่ปลอดภัย บุคคลภายนอกห้ามเข้า เดินสายสัญญาณฝังผนัง ร้อยท่อ ป้องกันการตัดต่อสาย
- ทำบันทึกอุปกรณ์ทุกชิ้นไว้ รวมทั้งเก็บข้อมูล Serial ต่างๆ ของอุปกรณ์ และโปรแกรม เมื่อเกิดปัญหา สามารถใช้อ้างอิงทางกฎหมายได้

ป้องกันวิธีวิศวกรรมสังคม (ตีมตุ๋น)

บรรดาวิธีการเจาะแบบต่าง ๆ นั้น ไม่มีวิธีใดได้ผลดีเท่ากับวิธีการตีมตุ๋น เนื่องจากรูปแบบวิธีการไม่ตายตัว และหลากหลายมาก ในภาพยนต์เรามักจะเห็นแต่วิธีการทางเทคนิค ใช้ความสามารถทางคอมพิวเตอร์เจาะเข้าไป แต่ในชีวิตจริง วิธีวิศวกรรมสังคม (Social engineering) นั้น ถูกใช้บ่อยและมากที่สุด และมักจะมาในรูปของหน้าม้า หรือผู้เข้ามาติดต่องาน ลูกค้า อาจจะโทรศัพท์เข้ามาสอบถาม เก็บข้อมูล ซึ่งการป้องกันได้ แต่ไม่ทั้งหมด

- ป้องกันไม่ให้ผู้ที่เกี่ยวข้องกับงานจริง ๆ มายุ่งกับระบบ เมื่อต้องตามช่างเทคนิค หรือวางระบบเพิ่ม ต้องอยู่ภายในสายตาเสมอ
- มีระบบการเข้าออกสถานที่ที่เข้มงวดตรวจสอบได้ ใช้มาตรการทางจิตวิทยา เช่น ให้ทราบกันทั่วไปว่ามีการอัดเทปสนทนา หรือติดกล้องวงจรปิด แต่ไม่ต้องบอกว่ามีกี่ที่ที่ไหนบ้าง
- เอกสาร ไฟล์ ทุกชนิด ไม่ใช้แล้ว ต้องทำลายทิ้ง
- มีการแบ่งงาน และฝ่ายที่ชัดเจน ห้ามฝ่ายที่ไม่เกี่ยวข้องเข้าไปยุ่งกับคอมพิวเตอร์ หรือระบบของฝ่ายอื่นโดยไม่ได้รับอนุญาต
- ใช้ระบบบันทึกการเคลื่อนไหวทั้งหมดบนระบบเครือข่าย เช่น บน Windows NT/2000 คุณสามารถบันทึกการเข้าออกการใช้งาน เปิดปิดโปรแกรม copy แก้ไขไฟล์ และกิจกรรมอื่น ๆ ตลอดเวลา
- ทดสอบ และหาวิธีการที่จะเจาะเข้าสู่ระบบตลอดเวลา เพื่อหาช่องโหว่
- ฝึกอบรมพนักงานถึงวิธีการป้องกัน และชี้ให้เห็นรูปแบบต่าง ๆ ที่อาจเป็นไปได้ที่จะถูกบุกรุก
- ติดตั้งระบบตรวจจับผู้บุกรุก IDS (Intrusion detection system) หากมีงบประมาณล่ะก็ มีเป็นโปรแกรมขายหลายยี่ห้อ
- ตรวจสอบอุปกรณ์ ฮาร์ดแวร์ การเดินสาย ซอฟต์แวร์และระบบ ต่าง ๆ สม่ำเสมอ

ทั้งหมดนี้ก็เป็นเรื่องราวเกี่ยวกับระบบรักษาความปลอดภัย ซึ่งไม่ได้เป็นเรื่องไกลตัวเลย ผู้เสียหายอาจเป็นคุณเข้าสักวันหรือบางที ตอนนี้คุณอาจจะกำลังโดยแฮ็กอยู่ก็ได้